The Data Protection Act 2018 came into effect on 25 May 2018. It is the responsibility of line managers to ensure that all employees who handle personal data complete Data Protection training annually as part of their induction or annual development plan.

Where it is suspected that there has been a breach of the terms of the Act, or a failure to adhere to the Council’s Information Security Policy or Data Protection and Confidentiality Guidelines which are available on Inside Falkirk, the circumstances may be subject to an investigation under the terms of the Council’s Disciplinary policy.

The level of investigation/action will be determined on a case by case basis. However consideration should be given to whether or not the incident is the first breach of the terms of the Act/policies by the employee, the number of people affected and the sensitivity of the data shared/disclosed.

If there is a reasonable belief that the incident has been a genuine mistake and has limited impact, it is suggested that a Management Counselling meeting followed up by a letter would be sufficient. However if the breach is significant affecting a large number of people, relates to sensitive personal data or may result in the Council incurring a monetary penalty or other formal action from the Information Commissioner, then a formal disciplinary investigation may be appropriate.

If the incident is not the first involving the employee then it would be appropriate to instigate a formal investigation under the Council’s Disciplinary process.

The following list may be helpful in determining if informal action may be appropriate in the first instance, although repeated incidents may warrant disciplinary action:

- Carelessness or negligence in the storage, use or sharing of personal data for a limited number of employees or service users.
- Failure to follow the Council’s policy for the recording and/or storage of personal data.
How to Manage a Breach of Data Protection and Confidentiality

- Accidental unauthorised disclosure of personal information in breach of Council policy and data protection legislation.
- Disclosure of non sensitive information relating to a single individual.
- Failure to complete training.

More serious cases which may require a formal investigation under the terms of the Council’s Disciplinary policy include:

- Deliberate sharing or misuse of personal information or data affecting a large number of employees or service users.
- Sharing of sensitive personal information or data with external organisations, the public or colleagues in other service areas.
- Sharing of personal information or data to discredit an employee or service user.
- Persistent failure to adhere to the Council’s Policy and data protection legislation.
- Deliberate failure to respond to a request for information under the terms of the Data Protection Act.
- Negligence or loss of personal information or data affecting a large number of employees or service users.